AF
IFW

Practitioner's Docket No. 2337/107 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Martin A. Dorey

Application No.: 10/646,365 Group No.: 2181
Filed: August 22, 2003 Examiner: Kim, Harold J.
For: System, Device, and Method for Managing File Security Attributes
In a Computer File Storage System

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF CORRECTED SUMMARY OF THE CLAIMED SUBJECT MATTER

1. Transmitted herewith is a Corrected Summary of the Claimed Subject Matter submitted in response to the Notice of Non-Compliant Appeal Brief dated December 27, 2006.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is ***mandatory;*** *Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

■ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
■ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
□ as "Express Mail Post Office to Addressee"
Mailing Label No. ______________ **(mandatory)**

TRANSMISSION

□ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Signature

Date: January 26, 2007

Jeffrey T. Klayman
(type or print name of person certifying)

** Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

2. STATUS OF APPLICANT

This application is on behalf of a small entity.

3. FEE PAYMENT

The filing fee of $250.00 was paid on October 3, 2006.

4. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 19-4972.

Date: January 26, 2007

Jeffrey T. Klayman
Registration No. 39,250
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
U.S.
617-443-9292
Customer No. 02101

02337/00107 607533.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Martin A. Dorey	Docket No.:	2337/107
Appl. No:	10/646,365	Art Unit:	2181
File Date:	August 22, 2003	Examiner:	Kim, Harold J.

Invention: System, Device, and Method for Managing File Security Attributes In a Computer File Storage System

****

CERTIFICATE OF MAILING

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 26, 2007.

Jeffrey T. Klayman

****

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CORRECTED SUMMARY OF THE CLAIMED SUBJECT MATTER

In response to the Notification of Non-Compliant Appeal Brief dated December 27, 2006, and pursuant to MPEP 1205.03, Applicants respectfully submit the following corrected Summary of the Claimed Subject Matter for the above-referenced appeal.

Summary of Claimed Subject Matter

The present application relates to managing file security attributes in a computer file storage system supporting at least two file security models. A file is stored using a first file security model (e.g., UNIX). A client using a second file security model (e.g., Windows) accesses the file. A set of file security attributes in accordance with the second file security model is generated. The set of file security attributes includes a plurality of security identifiers (SID), including at least an owner SID and a group SID, that are derived from corresponding identifiers associated with the file in accordance with the first file security model. When the system is unable to map an identifier from the first file security model to an identifier for the second file security model, the generated SID includes both a map failure indicator and the corresponding identifier from the first set of file security attributes, such that the map failure indicator indicates that the identifier relates to the first file security model rather than to the second file security model. The map failure indicator therefore allows information about the map failure to be conveyed in the SID.

Independent claims 1, 16, and 31 clearly require a security identifier that includes separate map failure indicator and identifier components. Specifically, the claims expressly require "at least one map failure indicator" **AND** a "corresponding identifier." The description clearly shows that the SID includes separate map failure indicator and identifier components. In fact, all of the exemplary embodiments described in the specification clearly include a distinct map failure indicator in addition to the identifier (e.g., a distinct UNIX-specific authority identifier along with the UNIX identifier in exemplary UNIX-specific SIDs shown at page 8, line 19 and page 19, line 15, and a distinct UNIX-specific indicator along with a UNIX identifier as qualifiers to a well-known authority identifier value in an alternative embodiment described at page 19, lines 25-28). Thus, the claims unequivocally require two separate and distinct components, namely a map failure indicator and an identifier.

Independent claim 1 is directed to a method for managing file security attributes by a file server in a computer file storage system, the computer file storage system including a file secured using a first file security model. The method involves receiving a first request from a client relating to the file stored in the computer file storage system, the client utilizing a second file security model (e.g., receive request from Windows client to read file security attributes in block 204 of FIG. 2); retrieving a first set of file security attributes, in accordance with the first file security model, associated with the file, the first set of file security attributes including at least an owner identifier and a group identifier (e.g., obtain file security attributes for the file in block 206 of FIG. 2); and generating a second set of file security attributes, in accordance with the second file security model, from the first set of file security attributes (e.g., blocks 210-216 shown in FIG. 2 and discussed in the application at page 10, line 17 – page 11, line 8), the second set of file security attributes including a plurality of security identifiers (SID) including at least an owner SID derived from the owner identifier (e.g., generate a Windows owner SID from the UNIX owner ID in block 210 of FIG. 2) and a group SID derived from the group identifier (e.g., generate a Windows group SID from the UNIX group ID in block 212 of FIG. 2), wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier from the first set of file security attributes (e.g., generate a UNIX-specific SID including the UNIX ID in block 312 of FIG. 3, which shows exemplary logic for generating a Windows SID from a UNIX ID, as discussed in the application at page 11, line 10 – page 12, line 21), wherein the map failure indicator indicates that said identifier relates to the first file security model (e.g., a distinct UNIX-specific authority identifier along with the UNIX identifier in exemplary UNIX-specific SIDs shown at page 8, line 19 and page 19, line 15, and a distinct UNIX-specific indicator along with a UNIX identifier as qualifiers to a well-known authority identifier value in an alternative embodiment described at page 19, lines 25-28).

Independent claim 16 is directed to an apparatus (e.g., file server 160 shown in FIG. 1 and discussed in the application at page 9, lines 8-9) for managing file security attributes in a computer file storage system, the computer file storage system including a file secured using a first file security model, the file associated with a first set of file security attributes including an owner identifier and a group identifier. The apparatus includes a network interface (e.g., block 802 shown in FIG. 8 and discussed in the application at page 18, lines 24-25) for communicating with clients over a communication network; a storage interface (e.g., block 806 shown in FIG. 8 and discussed in the application at page 18, lines 25-26) for communicating with a file storage device; and file security logic (e.g., block 804 shown in FIG. 8 and discussed in the application at page 18, line 26 – page 19, line 2, which performs such things as handling client requests, mapping between UNIX names and Windows names, generating and translating UNIX-specific SIDs, and translating UNIX file permissions into Windows file permissions) operating between the network interface and the storage interface for managing file security attributes. The file security logic includes logic for generating a second set of file security attributes, in accordance with the second file security model, from the first set of file security attributes (e.g., blocks 210-216 shown in FIG. 2 and discussed in the application at page 10, line 17 – page 11, line 8), the second set of file security attributes including at least an owner SID derived from the owner identifier (e.g., generate a Windows owner SID from the UNIX owner ID in block 210 of FIG. 2) and a group SID derived from the group identifier (e.g., generate a Windows group SID from the UNIX group ID in block 212 of FIG. 2), wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier from the first set of file security attributes (e.g., generate a UNIX-specific SID including the UNIX ID in block 312 of FIG. 3, which shows exemplary logic for generating a Windows SID from a UNIX ID, as discussed in the application at page 11, line 10 – page 12, line 21), wherein the map failure indicator indicates that said identifier relates to the first file security model (e.g., a distinct UNIX-specific authority identifier along with the UNIX identifier in exemplary UNIX-specific SIDs shown at page 8, line 19 and page 19, line 15, and a distinct UNIX-specific indicator along with a UNIX identifier as qualifiers to a well-known authority identifier value in an alternative embodiment described at page 19, lines 25-28).

Independent claim 31 is directed to a method involving receiving a security identifier (SID) including at least one map failure indicator and a corresponding identifier in accordance with a first file security model and translating the SID into a text string (e.g., with reference to FIG. 5, if Response with SD 508 includes a UNIX-specific SID, then the Windows client 120 sends a request 510 to file server 160 to translate the UNIX-specific SID, and the file server 160 sends a response 512 including a text string generated from the UNIX-specific SID – this is discussed in the application at page 15, line 21 through page 16, line 23).

Independent claim 30 is directed to a method for generating, from a first set of file permissions in accordance with a first file security model, a second set of file permissions in accordance with a second file security model (see, for example, page 12, line 23 through page 15, line 19 and FIG. 4 of the application). The method involves translating the first set of file permissions into the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions (see, for example, block 404 of FIG. 4 and page 12, line 23 through page 13, line 10); removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone (see, for example, block 406 of FIG. 4 and page 13, lines 16-18); adding any rights that need to be explicitly denied to the owner and to the group (see, for example, block 408 of FIG. 4 and page 13, line 18 through page 14, line 2); producing a set of access control elements ordered hierarchically (see, for example, block 410 of FIG. 4 and page 14, lines 4-18); and removing any redundant permissions from the access control elements (see, for example, block 414 of FIG. 4 and page 14, line 20 through page 15, line 6).

Independent claim 29 is being withdrawn from consideration.

Date: January 26, 2007

Respectfully submitted,

Jeffrey T. Klayman
Registration No. 39,250
Attorney for Applicant

Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
Ph.: (617) 443-9292
Fax: (617) 443-0004

02337/00107 603693.1